REMARKS

Claims 1-23 are pending and under consideration. Reconsideration is requested.

Traverse of Rejections

In items 3-7 of the Office Action, the Examiner rejects independent claims 1, 16-17, and 22-23 under 35 U.S.C. §103(a) as being unpatentable over Giniger et al. (U.S.P. 6199045) in view of Tatebayashi et al. (U.S.P. 6,009,174) and rejects dependent claims 2-15 and 18-21 under 35 U.S.C. §103(a) as being unpatentable over Giniger in view of Tatebayashi and combinations of Olsson (U.S. Pub. No. US 2002/0080968), Pirila (U.S.P. 6674860), and Walsh et al., Pub. No. US 2004/0033795. (Action at pages 2-20). The rejections are traversed.

Applicants submit that even an *arguendo* combination of the art of record does not teach features recited in each of the independent claims. Independent claim 1, for example, recites a system including:

a) "a terminal . . . encrypting . . . and transmitting the encrypted position information;"

b) "a position recording apparatus . . ., receiving the encrypted position information . . . and recording the encrypted position information. . .," and

c) "wherein the position recording apparatus can decrypt the previously recorded encrypted position information only after the terminal sends a key used to decrypt the previously recorded encrypted position information to the position recording apparatus and the position recording apparatus receives the key from the terminal (emphasis added)." Independent claims 16-17, and 22-23 have similar recitations.

Applicants submit that even an *arguendo* combination of the art of record does not teach an encrypted position information is transmitted to, and recorded on a position recording apparatus before a key used for decryption of the recorded position information is transmitted to the position recording apparatus, as recited by claim 1 for example.

The Action concedes that Giniger does not teach this feature. (See, for example, page 3, lines 18-21). However, the Examiner asserts, however, that Tatebayashi teaches:

> [A] transmission apparatus . . . stores three secret keys, . . . selects one secret key from the secret keys, . . . generating a message M . . .indicating a secret key. . . generating a cryptogram by encrypting the generated message using the secret key,...generating a cryptogram by encrypting the message using the message itself as the secret key, and . . transmitting the cryptograms to the reception apparatus to indicate the selected secret key. . . .reception apparatus . . . generating decrypted data by decrypting the cryptogram using a secret key out of the three secret keys, and . . . generating decrypted data by decrypting the cryptogram using the decrypted data, and authorizes that the secret key has been selected when the decrypted data matches the decrypted data . . . As can be read above, a

> transmission apparatus transmits a secret key to a reception apparatus. The secret key is used to decrypt or decipher. Combining . . . Tatebayashi . . . Giniger would result in a system wherein location information is measured, encrypted, and sent to a server. Using a secret key sent by the terminal, i.e., transmission apparatus, to the server, i.e., reception apparatus, the server decrypt the information.

(See, Action at page 4, lines 1 -16).

* * * * *

Applicants respectfully submit that the Examiner's interpretation of Tatebayashi is not correct and Tatebayashi does not teach that "a transmission apparatus transmits a secret key to a reception apparatus," as the Examiner asserts nor a transmission apparatus sent a key after recording position information. Rather, byy contrast, Tatebayashi merely teaches:

> In the present system, three secret keys K1, K2, and K3 are provided beforehand to the transmission apparatus 100 and to the reception apparatus 200, so that the transmission apparatus 100 can freely select one of these secret keys and use it to encrypt a digital production which it then transmits to the reception apparatus 200.

(Emphasis added, see, for example, col. 3, lines 40-46).

That is, Tatebayashi merely teaches that both the transmission apparatus 100 and the reception apparatus 200 have stored secret keys i.e., secret keys Kl, K2, K3 before the transmission of the messages. In further detail, Tatebayashi discloses operation of an transmission apparatus as:

> [S]ecret key selection unit 104 randomly selects one of the three secret keys K1, K2, or K3 stored in the secret key storage unit 103 . . . uses the secret key Ks to encrypt the block data . . . generating the cryptogram Cd . . sends this to the transmission unit 110 (step S11). . . .message generation unit 106 generates one message M (step S12). . . . uses the same secret key Ks to encrypt the message M . . . The encryption module 102 then sends this to the transmission unit 111. Meanwhile, the encryption module 107 encrypts the message M using the message M itself as the secret key, thereby generating the cryptogram Cm which it sends to the transmission unit 112 (step S13).

(See, for example, Fig. 2, and col. 7, lines 33-59).

That is, Tatebayashi merely teaches that a transmission apparatus 100 sends a first encrypted message encrypted by one of the stored secret keys and a second encrypted message to indicate the selected secret key. Further, Tatebayashi teaches, in particular, regarding the reception apparatus:

> [R]eception units . . . receive the three cryptograms Cd, Ca, and Cm transmitted from the transmission apparatus . . . decrypts the cryptogram Ca sent from the reception unit 211 using the secret key K1 read from the secret key storage unit 220 to generate the decrypted data M1. . . Simultaneously . . ., decrypts the cryptogram Ca sent from the reception unit 211 using the secret key K2 read from the secret key storage unit 230 to generate the decrypted data M2 . . .decrypts the cryptogram Ca sent from the reception unit 211 using the secret key K3 read

> from the secret key storage unit 240 to generate the decrypted data M3 In the second decrypting stage, . . . decrypts the cryptogram Cm received from the reception unit 212 using the decrypted data M1 generated by the decryption module 221 . . . judges whether the decrypted data M1 . . .matches the decrypted data M11 . . and so gives an indication . . indicating a selection of the secret key K1. As a result, . . . uses the secret key K1 sent from the secret key selection unit 202 to decrypt the cryptogram Cd.

(See, for example, Fig. 3 and col. 7, line 60 - col. 8, line 60).

That is, Tatebayashi teaches that the reception apparatus decrypts the first and second encrypted message by the three secret keys and recognizes the selected secret key by determining whether two decrypted messages match.

Accordingly, Tatebayashi teaches a reception apparatus 100 (*arguendo* a position recording apparatus) that previously stores the secret keys to decrypt the message. Thus, Tatebayashi teaches a reception apparatus that inherently can decrypt the data stored in the reception apparatus before the transmission apparatus sends the secret key.

Therefore, Tatebayashi does not disclose that "the position recording apparatus can decrypt the recorded encrypted position information only after the terminal sends the decryption data...," as recited by claim 1, for example.

Applicants point out that an advantage of the exemplary embodiment of the present invention is a protection a privacy of a position of a mobile terminal user from unauthorized access to the position recording apparatus in addition to prevent the interception during the communication. But, an arguendo combination of the art of record merely teaches encrypting a communication between a transmission side and a reception side to prevent interception during the communication.

Applicants submit that nothing in the teachings of Olsson, Pirila, nor Walsh cures the deficiencies argued above.

Claims 2-15 and claims 18-21 depend respectively from independent claims 1 and 17, which, for reasons argued above, patentably distinguish over combinations of the art of record.

Further, Applicants submit this traversal meets the Consideration of Applicant's Rebuttal Evidence Examination Guidelines for Determining Obviousness Under 35 U.S.C. §103 in View of the Supreme Court Decision in *KSR* International Co. v. Teleflex Inc. of October 3, 2007 and the elements in combination do not merely perform the function that each element performs separately, and the results of the claimed combination were unexpected.

Summary

Since features recited by independent claims 1, 16-17, and 22-23 (and respective dependent claims) are not taught by an *arguendo* combination of the art relied on by the Examiner, the rejections should be withdrawn and claims 1-23 allowed.

Conclusion

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: November 18, 2005

By: Paul W. Bobowiec

Paul W. Bobowiec
Registration No. 47,431

1201 New York Avenue, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501